AMPLÍA – REITERA – SOLICITA

Señor Fiscal Federal:

Javier Lorenzo Carlos Smaldone, DNI N.º [redacted], con el patrocinio de mi abogado defensor Pablo Slonimsqui, en autos caratulados "N.N. Y OTROS S/VIOLACIÓN DE CORRESPONDENCIA, INTIMIDACIÓN PUBLICA Y VIOLACIÓN SIST. INFORMÁTICO ART. 153 BIS 1° PÁRRAFO DENUNCIANTE: LA ROCCA, MARIO Y OTROS", expediente Nº 55276/2019 que tramitan ante el Juzgado Nacional en lo Criminal y Correccional Federal N° 9, Secretaría N° 18, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), respetuosamente digo:

AMPLÍA

Que en el escrito presentado en fecha 1 de marzo de 2021 por esta parte se hicieron notar las llamativas omisiones de la denuncia presentada el 30 de julio de 2019 por personal de la Policía Federal sobre los hechos de marras, que se limitó a manifestar la vulneración de tres (03) cuentas de Gmail en uso por dicha fuerza. En dicho escrito se destacó que el acceso indebido al servidor *supbienestar.gob.ar* de la Superintendencia de Bienestar y su posterior modificación para realizar una maniobra de *"phishing"* no fueron reconocidos sino hasta luego de producida la filtración masiva de datos el 12 de agosto de 2019, conocida popularmente como *"La Gorra Leaks 2.0"*. También se hizo alusión a la resolución RESOL-2020-30-APN-AAI de la Agencia de Acceso a la Información Pública[1], según la cual en el informe IF-2019-80081802-APN-SCIB#PFA de la Policía Federal se reconocía que: "*la información (vulnerada) fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmail"*. Respecto de esto último es que quisiera darle algunas precisiones técnicas y consideraciones con la esperanza de contribuir a su mejor comprensión de los hechos, desde mis más de veinticinco años de experiencia en la instalación, el mantenimiento y el soporte de servidores informáticos como los aquí involucrados.

El software PHP (un lenguaje de programación, de los más utilizados en la *World Wide Web*) en su versión 5.6.3 fue publicado el 14 de noviembre de 2014[2] (y la siguiente versión, 5.6.4, el 18 de diciembre de 2014). A mayo de 2016 ya existían al menos cuatro (04) vulnerabilidades graves detectadas, documentadas, publicadas y explotables[3]. Esto significa que al momento de

1 https://www.argentina.gob.ar/sites/default/files/rs-2020-30-apn-aaip.pdf
2 https://www.php.net/releases/index.php
3 https://cvedetails.com/vulnerability-list.php?vendor_id=74&product_id=128&version_id=178179&order=3

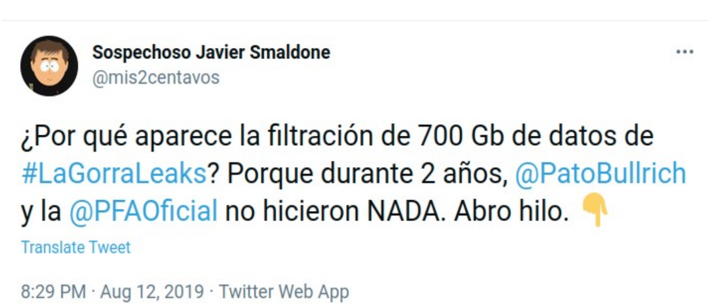
detectarse la intromisión en el servidor *supbienestar.gob.ar*, el 28 de julio de 2019, hacía ya más de tres años que cualquier persona con modestos conocimientos en la materia podría haber realizado una maniobra similar a la que, esta vez, tomó estado público.

Es realmente alarmante pensar que la institución policial alojaba información confidencial en un servidor en semejante estado de abandono. No se entiende cómo no se tomaron medidas para solucionar problemas de seguridad graves documentados y publicados en mayo de 2016. Bastaba para esto con una simple actualización del software PHP, tarea rutinaria para cualquier profesional en la materia y que no demanda más que unos minutos.

La aplicación de actualizaciones de seguridad es una tarea crucial en el mantenimiento de servidores, y es realmente crítica en el caso de aquellos expuestos a Internet (como es el caso de *supbienestar.gob.ar*). Es una práctica común y bien establecida en la industria la actualización de servidores de forma semanal o, a lo sumo, mensual. Y en el caso de publicarse vulnerabilidades graves (como las descubiertas en PHP 5.6.3 en mayo de 2016), debe realizarse tan rápido como sea posible. Por otra parte, cualquier administrador de sistemas de este tipo sabe que PHP es un constante vector de ataques (que ha posibilitado filtraciones de datos importantes, como la que nos ocupa) ya que regularmente se encuentran en él errores y vulnerabilidades que deben ser corregidas.

Es realmente alarmante que ni siquiera se revisara la seguridad de dicho servidor y se actualizara el componente de software defectuoso luego de que en mayo de 2017 se produjera la primera filtración de datos de la Policía Federal, conocida como *"La Gorra Leaks"*. En aquella ocasión esta parte contribuyó a denunciar el hecho ocurrido aportando prueba en el marco de la causa Nº 1033/2017 del Juzgado Nacional en lo Criminal y Correccional Federal Nº 2 y prestando luego declaración testimonial. Esto motivó una denuncia realizada por la Fiscalía Nacional en lo Criminal y Correccional N° 10 el 5 de junio de 2017. Quizás esto explique la animosidad puesta de manifiesto por los investigadores policiales hacia mi persona.

Tan pública y notoria fue la inacción policial ante el hackeo y posterior filtración de mayo de 2017 que, al tomar estado público la filtración ocurrida el 12 de agosto de 2019, expresé lo siguiente en la red social Twitter[4]:



4 https://twitter.com/mis2centavos/status/1161057262321983488

En dicho tweet —y en el hilo que de él se desprende— expliqué lo que hoy, a la luz de la evidencia resumida en este escrito, aparece claro: que la nueva filtración se produjo porque ni se investigó debidamente ni se tomaron las medidas de seguridad adecuadas luego de la primera filtración de información de la Policía Federal Argentina. Es notable que ni este tweet, ni los que le siguen a continuación, fueran citados ni por los informes policiales de “ciberpatrullaje” de fs. 199-231 —donde aparecen once (11) tweets míos emitidos por esos días— ni en el “ANEXO 4” de fs. 515-532, exclusivamente dedicado a mi persona —donde aparecen cincuenta y siete (57) tweets míos emitidos en distintos momentos a lo largo de más de ocho (08) años.

Dado que tanto al realizar la denuncia como al ratificarla se ocultó lo sucedido con el servidor *supbienestar.gob.ar,* y solo se reconoció luego de hacerse evidente al tomar estado público el contenido de los archivos filtrados, cabe preguntarse además si este fue el único servidor vulnerado en dicha oportunidad y cuántos otros se encontraban en similar estado de incuria.

Es llamativo también que en ningún informe policial incluido en el expediente muestre que se haya analizado en detalle la naturaleza de la información filtrada, ni siquiera su volumen, lo que resultaría esencial para determinar el origen de la misma y el impacto y posibles consecuencias de los hechos ocurridos.

Para finalizar, recordemos que la Agencia de Acceso a la Información Pública en la resolución del 5 de febrero de 2020 antes citada aplicó sendos apercibimientos a la Policía Federal Argentina por haber incumplido los deberes de seguridad (artículo 9) y de confidencialidad (artículo 10) de la Ley N° 25.326.

En definitiva:

- El servidor *supbienestar.gob.ar* de la Superintendencia de Bienestar de la Policía Federal tenía un componente de software sin actualizar (PHP) aproximadamente desde **diciembre de 2014**.
- Dicho software tenía vulnerabilidades graves que eran públicas desde **mayo de 2016**.
- Desde ese momento, cualquier persona con mínimos conocimientos podía explotar dichas vulnerabilidades y acceder a la información confidencial alojada en el servidor.
- No se tomaron medidas para solucionar dichas vulnerabilidades luego de ocurrida la filtración de datos de la Policía Federal (*“La Gorra Leaks”*) en **mayo de 2017**.
- Dichas vulnerabilidades seguían presentes en el servidor y fueron explotadas para realizar una maniobra de *“phishing”* (que derivó en el compromiso de tres cuentas de correo electrónico) el **28 de julio de 2019**.
- No se hizo referencia alguna a estas vulnerabilidades, ni al acceso ilegítimo al servidor *supbienestar.gob.ar*, ni alteración del mismo, en los informes policiales previos a la

denuncia realizada por la Policía Federal de forma telefónica el **30 de julio de 2019** (fs. 17) y ratificada en el juzgado el **13 de agosto de 2019** (fs. 31-32).

- En la denuncia inicial el personal policial dijo que los datos filtrados (*"La Gorra Leaks 2.0"*) —entre 259 GB y 700 GB, según las fuentes periodísticas— provenían de tres (03) cuentas de Gmail comprometidas, que en conjunto pueden almacenar solo 45 GB.
- La Policía Federal dijo a la Agencia de Acceso a la Información Pública que la filtración se produjo por la vulneración del servidor *supbienestar.gob.ar,* debida a los problemas de seguridad del software PHP no solucionados, y que <u>la información (vulnerada) fue obtenida del mismo</u>. Fue sancionada por esta última el **5 de febrero de 2020**.

REITERA - SOLICITA

En razón de lo expuesto, reitero mi pedido de que se investiguen las notorias omisiones por parte de la Policía Federal Argentina en la denuncia y la investigación de los hechos acontecidos.

Pido también se solicite a la Agencia de Acceso a la Información Pública el expediente EX-2019-72366951- -APN-DNPDP#AAIP, que motivara la resolución RESOL-2020-30-APN-AAIP, incluyendo el informe IF-2019-80081802-APN-SCIB#PFA aludido en la misma ad effectum videndi et probandi.

Además, solicito se extraigan testimonios de la causa Nº 1033/2017, que tramita en el Juzgado Nacional en lo Criminal y Correccional Federal Nº 2, a fin de determinar si a raíz de la filtración ocurrida y denunciada en mayo de 2017 se emitieron alertas a la Policía Federal respecto del nivel de seguridad de sus servidores y qué medidas tomó la fuerza policial en consecuencia.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone